

WE CLAIM:

1 1. A method for establishing a secure connection between a client platform
2 and a service, comprising:
3 downloading a digitally signed applet from the service to the client platform;
4 verifying the digitally signed applet at the client platform using a first public
5 key the client platform already knows and trusts;
6 executing the applet at the client platform, thereby controlling the client
7 platform to store a second public key corresponding to the server; and
8 using the stored second public key to authenticate the service and establish
9 the secure connection.

1 2. The method of claim 1 wherein the applet includes first program code
2 that controls the client platform to store the second public key to a non-volatile
3 memory.

1 3. The method of claim 2 wherein the non-volatile memory comprises disk.

1 4. The method of claim 2 wherein the applet further includes second
2 program code that controls the client platform to use the stored second public key
3 to verify a signature subsequently provided by the server.

1 5. The method of claim 1 wherein the applet further includes program code
2 that controls the client platform to use the stored second public key to verify a
3 signature subsequently provided by the server.

1 6. The method of claim 1 wherein the executing step includes controlling
2 the client platform to store a second public key in the form of a digital certificate
3 corresponding to the server, and the using step comprises receiving a digital
4 signature from the server, and authenticating the received digital signature under
5 control of the executing applet through use of the stored digital certificate
6 corresponding to the server.

1 7. The method of claim 1 wherein the using step includes having the
2 executing applet invoke a further applet to establish a secure connection.

1 8. The method of claim 1 wherein the applet comprises a signed Java
2 Archive containing a digital certificate corresponding to the server, and a program
3 fragment that stores the digital certificate in a predetermined location on the client
4 platform that permits the client platform to later retrieve the stored digital
5 certificate.

1 9. A client platform for establishing a secure connection with a service over
2 a network, comprising:

3 an applet receiver that receives a digitally signed applet from the service
4 over the network;

5 an applet verifier that verifies the digitally signed applet using a first public
6 key the client platform already knows and trusts;

7 an applet executor that executes the applet, thereby controlling the client
8 platform to store a second public key corresponding to the server, and uses the
9 stored second public key to authenticate the service and establish the secure
10 connection.

1 10. A method for establishing a secure connection with a client, comprising:

2 downloading an applet to the client platform, the digitally signed applet
3 being digitally signed such that the client platform can verify the digitally signed
4 applet using a first public key the client platform already knows and trusts, the
5 digitally signed applet including a second public key and code that controls the
6 applet to store the second public key on the client platform;

7 sending a digital credential to the client, said digital credential being
8 verifiable by the client platform using the stored second public key; and

9 establishing a secure communication with the client based on said digital
10 credential as verified by the client.

1 11. The method of claim 10 wherein the applet code controls the client
2 platform to store the second public key to a non-volatile memory.

1 12. The method of claim 11 wherein the non-volatile memory comprises
2 disk.

1 13. The method of claim 10 wherein the applet further includes further code
2 that controls the client platform to use the stored second public key to verify the
3 digital credential.

1 14. The method of claim 10 further including sending a further applet to the
2 client platform in response to an invocation of the further applet by the first-
3 mentioned applet.

1 15. The method of claim 10 wherein the applet comprises a signed Java
2 Archive containing a digital certificate, and a program fragment that stores the
3 digital certificate in a predetermined location on the client platform that permits the
4 client platform to later retrieve the stored digital certificate.

1 16. A server for establishing a secure connection with a client over a
2 network, comprising:

3 an applet transmitter that transmits a digitally signed applet to the client
4 over the network, the applet being digitally signed using a first public key the
5 client already knows and trusts, the applet including a program that controls the
6 client to store a second public key corresponding to the server; and

7 a digital credential transmitter that transmits a digital credential to the client
8 executing the applet, the digital credential being authenticatable by the second
9 public key.

- 1 17. A method for establishing a secure connection between a server and a
2 web browser having access to a first, trusted public key, comprising:
3 downloading a digitally signed item from the server to the browser, the item
4 including a second public key;
5 verifying the digitally signed item at the browser using the first public key;
6 storing the second public key in response to the verifying step; and
7 using the stored second public key to authenticate the server.
1 18. A method as in claim 17 wherein the item comprises a Java archive.